Raspodijeljene glavne knjige i kriptovalute

Alternativni pristupi rudarenju

Ante Đerek, Zvonko Konstanjčar

14. studenoga 2021.

Strategije i inicijative rudarenja

Kod sastavljanja bloka, rudari moraju odlučiti

- Koje transakcije uključiti u blok? (standardna strategija: sve koje nude transakcijske provizije iznad nekog praga)
- Na kojem bloku graditi lanac? (standardna strategija: na najduljem lancu)
- Koji od dva bloka odabrati, ako stignu u približno istom trenutku? (standardna strategija: onog za kojeg su prvo čuli)
- Kada objaviti novi blok? (standardna strategija: odmah nakon pronalaska odgovarajućeg *nonce*)

Većina rudara slijedi standardne strategije, no jesu li one najisplativije?

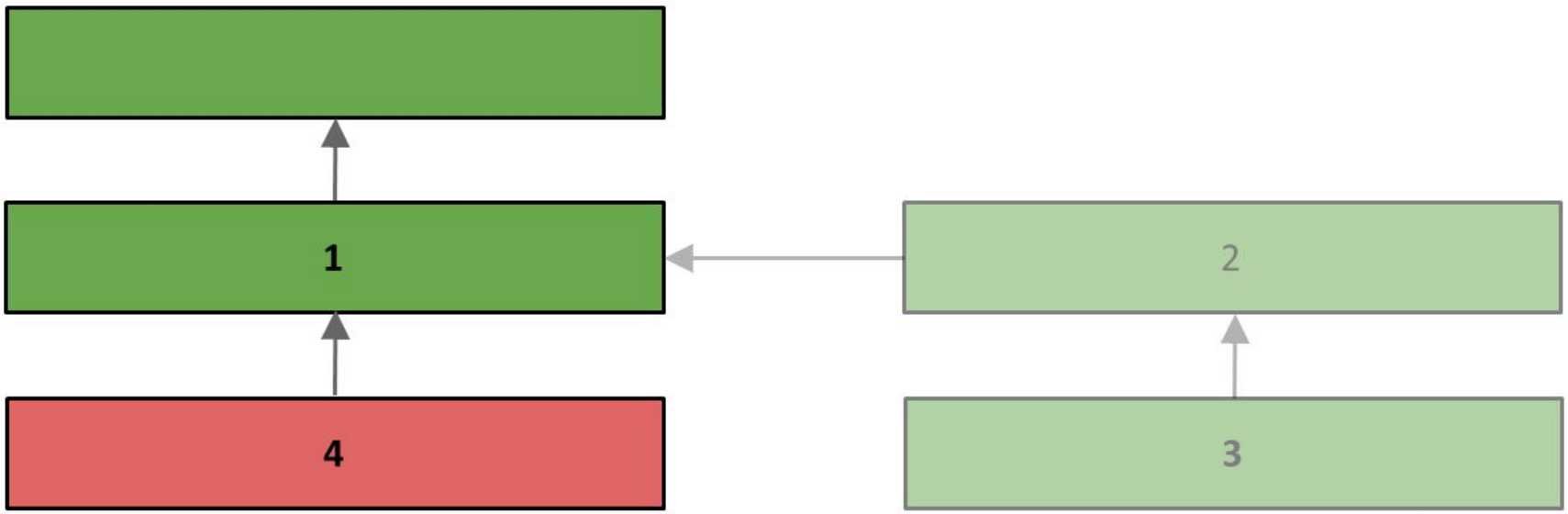
Strategije i inicijative rudarenja

Neke potencijalno isplative (ne)standardne strategije.

Pretpostavka: postoji rudar koji kontrolira postotak α ukupne rudarske snage.

- Forking napad
  - potrebno $\alpha > 0.5$
  - vjerojatno bi srušio vrijednost Bitcoina (kroz burze)
- Forking napad kroz podmićivanje
  - direktno podmićivanje ciljanih rudara
  - izgradnja novog bazena rudara te financiranje njega dok fork ne uspije
  - ostavljati velike "nagrade" u blokovima koji su u forking lancu
- Privremeno zadržavanje blokova
  - sebično rudarenje
  - dovoljno $\alpha > 0.33$, vrlo vjerojatno dovoljno i $\alpha > 0.25$

Strategije rudarenja - privremeno zadržavanje blokova



Izvor: `bitcoinbook.cs.princeton.edu`

Glavni problem svih ovih nestandardnih strategija je transparentnost mreže i posljedično potencijalno pad vrijednosti Bitcoina.

Glavni problemi proof-of-work Bitcoin sustava

- **Ogromna potrošnja energije**
- **Rudarenje se svelo na nekoliko velikih bazena (ASIC) - opasnost od preuzimanja mreže**

Alternativni pristupi rudarenju - zahtjevi na slagalice

Nužna svojstva:

- Provjera rješenja mora biti brza i učinkovita (svi čvorovi provjeravaju rješenje)
- Težina slagalica bi se trebala moći mijenjati (ako se mreža poveća ili smanji)
- Vjerojatnost nalaženja rješenja u svakom vremenskom intervalu trebala bi ovisiti isključivo o količini korištenih resursa u tom intervalu - odsustvo memorije (veći rudari bi trebali imati samo proporcionalno veću šansu za rješavanje slagalice)

Poželjna svojstva:

- Slagalica bi trebala biti otporna na ASIC
- Za rješavanje ne bi trebalo trošiti puno energije

Slagalice otporne na ASIC

Problemi:

- Trenutno mala grupa profesionalnih rudara kontrolira proces Bitcoin rudarenja - mnogi smatraju da je to opasno
- U originalnom radu od Satoshi Nakamota piše: "jedan-CPU-jedan-glas"
- Inicijalno Bitcoin je zamišljen kao demokratski sustav u vlasništvu svih članova

Ideja:

- Sagraditi slagalice nad kojima specijalizirani hardver ne bi bio prednost - utopija
- Realnije - slagalice nad kojima specijalizirani hardver ne bi donosio toliku prednost

Slagalice otporne na ASIC

Pristupi:

- Slagalice za koje je potrebno puno memorije ("memory hard" + "memory bound")
  - Scrypt (implementiran u Litecoinu - pokazalo se da nije otporan na ASIC)
- X11 - kombinacija 11 različitih hash funkcija - koristi se u altcoinu DASH
- Meta koja se giba - slagalica se mijenja

Postoje i protuargumenti koji zagovaraju ostanak na SHA 256 slagalici - riskantan prelazak na kriptografski slabije slagalice - potencijalni sigurnosni problemi.

- Pokazalo se da se ASIC sustavi ne grade za altcoine male tržišne vrijednosti - u ranim fazama je zlatni period CPUa i GPUa

Proof-of-Useful-Work

IDEJA: Možemo li složiti slagalicu kod koje se energija potrebna za njeno rješavanje može iskoristiti za korisne stvari u društvu. Ekološki, financijski i politički to bi to bilo jako poželjno.

Postoji povijest raspodijeljenih računalnih projekata.

Project	Founded	Goal	Impact
Great Internet Mersenne Prime Search	1996	Finding large Mersenne primes	Found the new "largest prime number" twelve straight times, including $2^{57885161} - 1$
distributed.net	1997	Cryptographic brute-force demos	First successful public brute-force of a 64-bit cryptographic key
SETI@home	1999	Identifying signs of extraterrestrial life	Largest project to date with over 5 million participants
Folding@home	2000	Atomic-level simulations of protein folding	Greatest computing capacity of any volunteer computing project. More than 118 scientific papers.

Izvor: `bitcoinbook.cs.princeton.edu`

Koji bi projekt mogao poslužiti kao slagalica?

Izazovi oko Proof-of-Useful-Work

- Imamo li uniforman prostor rješenja? npr. kod projekta SEFI@home moguće je da na određenim segmentima signala je moguće s većom vjerojatnošću detektirati anomalije.
- Imamo li neprebrojiv skup slagalica? npr. kod SEFI@home imamo konačan skup podataka za analizu.
- Imamo li slagalice koje se algoritamski generiraju? Kod SEFI@home određeni administratori generiraju podatke i definiraju cilj potrage.

Očigledno od ponuđenih otpadaju SEFI@home i Folding@home, možda Mersenne Prime Search - problem jer ne možemo kontrolirati težinu slagalice (svega 14 brojeva je nađeno u 18 godina)

Proof-of-Useful-Work - Primecoin

Jedan od implementiranih *Proof-of-Useful-Work* sustava je **Primecoin** kriptovaluta.

- Zasnovan na Cunninghamovom lancu - niz od k prostih brojeva $p_1, \ldots, p_k$, tako da vrijedi $p_i = 2p_{i-1} + 1$ za svaki broj u lancu,
- Za sada najdulji lanac je duljine 19 (pronađen 2014. godine, Jaroslaw Wroblewski),
- Postoji konjektura prema kojoj postoji Cunninghamovom lanac duljine k, za svaki k,
- Upitna korisnost.

Proof-of-Useful-Work - Proof-of-storage

IDEJA: kreirati slagalicu kojom treba pohraniti veliku količinu podataka za izračunavanje.

Primjer je Permacoin (Zajednički rad Sveučilišta Maryland i Microsofta).

- Kreće se od velike datoteke F (čiji sadržaj svi znaju) - idealno datoteka koja ima neku javnu vrijednost, npr. eksperimentalni podatci iz velikog hadronskog sudarivača - nekoliko stotina PB (backup za te podatke je korisna stvar).
- Organizirati datoteku u Merkleovo stablo (svi se trebaju složiti oko početnog hasha)
- Svaki rudar M sprema slučajan podskup $F_M \subset F$

Proof-of-Stake i virtualno rudarenje

IDEJA: zamijeniti računalne slagalice s virtualnim rudarenjem (mali troškovi u vidu računalnih resursa).

Zatvaranje petlje: što ako Bitcoin ili neka druga kriptovaluta postane dominantno sredstvo plaćanja?

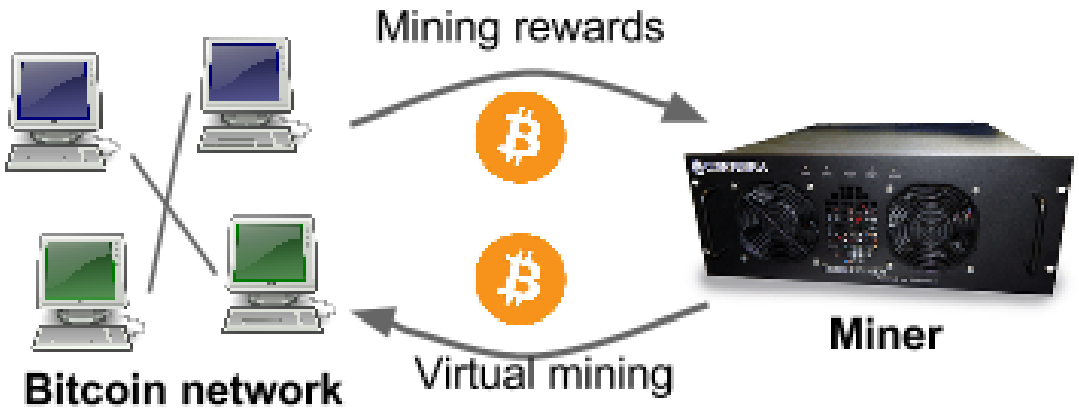
Izvor: `bitcoinbook.cs.princeton.edu`

U ravnoteži: svi ostvaruju približno jednake povrate na uloženi kapital. Oni koji više ulože u opremu više će i zaraditi.

Proof-of-Stake i virtualno rudarenje

IDEJA: treba li nam realni svijet?

- Ionako kroz realni svijet dokazujemo tko je najviše uložio u rudarenje
- Zašto ne alocirati snagu rudarenja direktno vlasnicima valute proporcionalno njihovom vlasništvu



Izvor: `bitcoinbook.cs.princeton.edu`

Inicijalna ideja Bitcoin rudarenja: glasanje proporcionalno računalnoj snazi.

Prednosti virtualnog rudarenja

- **Najvažnije**: ne trošimo energiju iz vanjskog svijeta
- Pozitivan utjecaj na okoliš
- Potrošnja energije ne pada na nulu - i dalje rudari provjeravaju transakcije i završavaju blokove
- Virtualno rudarenje je otporno na ASIC - svi rudari su jednako efikasni
- Svi vlasnici Bitcoina su rudari i **imaju motivaciju da mreža vrijedi što više**

Implementacija virtualnog rudarenja - Peercoin

NAPOMENA: ove ideje su dio aktivnog istraživanja

- **coin-age** - umnožak iznosa transakcije i broja blokova u kojima taj izlaz nije potrošen
- Rudarenje kod Peercoina je jednako kao i kod Bitcoina, samo što si rudari mogu prilagoditi težinu rudarenja ovisno o tome koliko žele coin-agea potrošiti.
- Blok sadrži posebnu coinstake transakciju
- Rudari mogu uložiti puno coin-age i malo računarske snage ili obrnuto
- Računalna snaga je ovdje primarno za slučajeve kada imamo više rudara s približno jednakim coin-ageima (da se osigura slučajnost)
- Sličan dizajn prisutan je kod: Nxt, BitShares, BlackCoin, Reddcoin

Proof-of-stake

- Rudarenje je lakše za one koji posjeduju više valute
- Slično kao i proof-of-coin-age, ali starost coina nije važna
- coin-age se kod proof-of-coin-age nakon uspješnog rudarenja resetira
- Kod proof-of-stake najbogatiji imaju uvijek najlakši zadatak - potencijalni problem

Proof-of-deposit

- Nakon što se određeni coinovi iskoriste za rudarenje bloka oni ostaju zamrznuti određen broj blokova
- Suprotno od coin-agea, ovdje rudar ne smije koristiti coinove određen period u budućnost
- U oba slučaja ulog efektivno dolazi od oportunitetnog troška da se coinovi određen period ne koriste za druge akcije

Proof-of-stake - nothing-at-stake problem

- Pretpostavimo da napadač s udjelom $\alpha < 50\%$ uloga pokuša napraviti fork od k blokova
  - Takav napad neće uspjeti s velikom vjerojatnošću (eksponencijalno raste s k)
  - U tradicionalnom rudarenju takav pokušaj ima veliki oportunitetni trošak (mogao je rudariti nad dobrim blokovima i potencijalno zaraditi nagradu)
- Kod virtualnog rudarenja nema oportunitetnog troška
  - Rudar može koristiti svoj ulog za rudarenje na najduljem lancu, ali istodobno može probati kreirati fork
  - Racionalno ponašanje je konstantno pokušavati razne forkove
- Uvode se razni pokušaji sprečavanja toga - kontrolne točke za sprečavanje dugačkih forkova
- Kod Etehereuma je uveden mehanizam kažnjavanja pokušaja forka (Slasher)

Proof-of-stake - ostali problemi

- Općenito virtualno rudarenje olakšava razne vrste napada
- Npr. postaje jednostavno udruživanje coin-stakeova kako bi se ubrzalo rudarenje pa i kreirali forkovi
- Ako neki rudar uspije kontrolirati $> 50\%$ uloga, tada on može tu situaciju zadržati u nedogled (rudari samo nad svojim blokovima) i u konačnici postaje vlasnik mreže
- U tradicionalnom rudarenju, uvijek je postojala šansa da netko kupi moćniju opremu

Proof-of-stake - perspektiva

- Za sada još nije jasno hoće li to uspjeti
- Postoji argument prema kojem sigurnost zahtijeva trošenje realnih resursa
- U tom kontekstu potrošnja energije u proof-of-work sustavu odgovara troškovima sigurnosti mreže
- Njie ništa dokazano - puno istraživanja i poslovnih eksperimenata